A THREE-FACTOR AUTHENTICATION MODEL FOR IMPROVED SECURITY

BY

OLU FELIX OLUTIMI
REG. NO: UNN/DBI/PG/UD/MSc/07/83

DEPARTMENT OF ELECTRONIC ENGINEERING

UNIVERITY OF NIGERIA, NSUKKA

FEBRUARY 2016

UNIVERSITY OF NIGERIA

TO RESTORE THE DIGNITY OF MAN

TITLE PAGE

A THREE-FACTOR AUTHENTICATION MODEL FOR IMPROVED SECURITY

BY

OLU FELIX OLUTIMI

REG. NO: UNN/DBI/PG/UD/MSc/07/83

DEPARTMENT OF ELECTRONIC ENGINEERING

FACULTY OF ENGINEERING

UNIVERITY OF NIGERIA, NSUKKA

APPROVAL PAGE

A THREE-FACTOR AUTHENTICATION MODEL FOR IMPROVED SECURITY

BY

OLU FELIX OLUTIMI
REG. NO: PG/UD/MSc/07/83

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF DEGREE OF MASTER OF ENGINEERING (M. ENG) IN THE DEPARTMENT OF ELECTRONIC ENGINEERING, DIGITAL COMPUTER OPTION, UNIVERSITY OF NIGERIA NSUKKA.

OLU FELIX OLUTIMI SIGNATURE ……….. DATE ……….
(STUDENT)

PROFESSOR A.N. NZEAKO SIGNATURE ……….. DATE ……….
(SUPERVISOR)

EXTERNAL EXAMINER SIGNATURE ……….. DATE ……….

DR M.A. AHANEKU SIGNATURE ……….. DATE ……….
(Ag. HEAD OF DEPARTMENT)

PROFESSOR W.I. OKONKWO SIGNATURE …………. DATE …….
(CHAIRMAN, FACULTY
POSTGRADUATE COMMITTEE)

CERTIFICATION

Olu Felix Olutimi, a master's degree postgraduate student in the Department of Electronic Engineering, University of Nigeria, Nsukka and with registration number **UNN/DBI/PG/UD/MSc/07/83** has satisfactorily completed the requirements for the award of Master of Engineering (M. ENG) in Information and Communications Technology Specialisation.

----------------------------------	-----------------------------------
PROF. A.N. NZEAKO	DR. M.A. AHANEKU
(SUPERVISOR)	(Ag. HEAD OF DEPARTMENT)

PROFESSOR W.I. OKONKWO
(CHAIRMAN, FACULTY POSTGRADUATE COMMITTEE)

DECLARATION

I, **OLU FELIX OLUTIMI**, a postgraduate student in the Department of Electronic Engineering, University of Nigeria, Nsukka, declare that the work embodied in this thesis is original and has not been submitted by me in part or in full for any other diploma or degree of this or any other university.

____________________ ________________________

OLU FELIX OLUTIMI **DATE**

UNN/DBI/PG/UD/MSc/07/83

DEDICATION

This project thesis is dedicated to the Glory of the Almighty God, who in spite of all odds and hopelessness, made this work to be successful.

ACKNOWLEDGEMENT

This work will be incomplete if the persons due are not acknowledged appropriately. I want to recognise the Grace of God that made me fit and favoured to complete the work. I give glory to God for that, immensely. The cooperations of lecturers who were available to teach, guide and correct my lectures and assignments is highly recognised. I thank the staff of Digital Bridge Institute for all their efforts towards a successful completion of the programme especially the tireless Mrs Taiwo Adeyemi.

The opportunity given me by the management of my office, the Energy Commission of Nigeria cannot be ignored at all. I thank the Management. I appreciate also Dr A.M. Umar, who supervised my Internship, as well as my project supervisor, Professor A. N. Nzeako, for his elderly guide. I cannot fail to recognise the tireless encouragement and cooperations I received from the Head of Department, Electronics Engineering, Professor C.I. Ani.

Finally, not in the least at all, I thank my family, especially my dear wife, Mrs Comfort F. Olu, for the prayers they kept saying to God, for a successful completion of this programme. I love you.

OLU, FELIX OLUTIMI
FEBRUARY 2016

ABSTRACT

Cloud computing has not only emerged as an accepted computing paradigm, but is fast penetrating into major sectors of human endeavor. These include banking, human resources management, justice administration, investigation, academia/research, commerce, health administration etc. Based on the public and experts concerns about cloud applications in the mentioned sectors, preliminary investigations were carried out and it was found that security, and in particular, authenticating cloud users is the biggest challenge to cloud computing. Technologies employed by experts to resolve this challenge include the one, two, or three-factor authentications. Studies showed that the first two technologies are in vogue, but little use has been made of the three-factor model. This work therefore investigates the use of three-factor authentication model, developed an option of it and developed a Mat Lab code for it based on a pseudo code; adding more options to cloud security and providing a benchmark to assure the effectiveness of the option. The investigation also discovered and collated more knowledge for further research in the subject matter. Results of this research showed through probability analyses, that the three-factor model will appreciably reduce the chance (probability) of guessing the parameters to access a cloud system (and any network indeed) and greatly increase the randomness (entropy) of such attempts.

Keywords: Cloud, Security, Authentication, Factors, Probability, Entropy

TABLE OF CONTENT

LIST OF TABLES AND FIGURES

Chapter 1

INTRODUCTION

1.1 Background of Study

In network architectures, it is possible to provide computer network in such a way that a client accesses computing resources such as application software packages, storage space, access to other networks, utilization of extra memory, computing speed or extra processor including infrastructure on which they operate, in a network. The client may not need to have so much resources in his computer than the very basic ones including a web browser, with which he would access the hosting network. He can store his completed job within the same provision. This scenario is called Cloud Computing. Web-based e-mail programs (Yahoo!, gmail, hotmail etc), present day web-based file storage (Google drive), facebook, twitter, Quickteller, Amazon, Jumia, Internet Banking and so on, are examples of cloud computing.

Cloud computing refers to the delivery of scalable IT resources over the Internet, as opposed to hosting and operating those resources locally, such as on a college or university network [50].

An organization can purchase these resources as the need arises, through the deployment of IT infrastructure and services over the network. It can then avoid the capital costs of software and hardware.

The client side of the architecture, consisting of the client's computer, its network as well as the application required to access the cloud computing system is termed front end. Examples of the application software for access include, Microsoft Internet Explorer, Mozilla Firefox, Google Chrome and all web browsers. The other end, back end, which is also referred to as the cloud, interacts with the front through a network, usually the Internet. It is made up of various computers, servers and data storage systems, with appropriate software packages. These create the "cloud" of computing services. Cloud computing is run by special software called middleware, using its own protocols. The middleware allows computers connected in the cloud to communicate with each other.

1.2 Benefits of Cloud Computing

Other benefits of cloud computing include the fact that clients would be able to access their applications and data from anywhere at any time. It could bring hardware costs down, since the need for advanced hardware on the client side will be reduced. Cloud computing saves companies the trouble of space for servers and digital storage devices, which may have to be rented. They have the option of storing their data on someone else's facility, which may reduce spending on IT support. It is common knowledge that the use of computers imposes the responsibility of purchasing licensed software packages on the owner, for each computer in use. For a large corporation, the savings in paying only metered fee to a cloud computing company or acquiring a centralized cloud computing facility with cheaper (bulk) license may be another significant benefit. According to Brian Gammage, a Gartner Fellow, moving data centre to a cloud provider will cost a tenth of the acquisition cost, and the use of cloud applications can reduce costs from 50% to 90% - CTO of Washington D.C.[33]. This gave birth to new businesses referred to as Cloud Services Providers (CSP).

If the cloud computing system's back end is connected in a grid computing pattern, the client could take advantage of the network's processing power. For instance a complex scientific calculation could be sent to such cloud for speedy output, by tapping into the processing power of all available computers on the back end.

Furthermore, cloud offers what is called multitenancy, where a provider shares resources between users at the same time, through virtualization. In the same vein, almost all resources being provided can be scaled, based on the current need and increased as the business grows. The offer is elastic, in that subscriptions can be up-scaled or downscaled as needed. Load balancers are usually employed to achieve this. For both users and CSPs, location of request, resources, users or provider does not matter, since the only requirement is access network and legitimate subscription parameters.

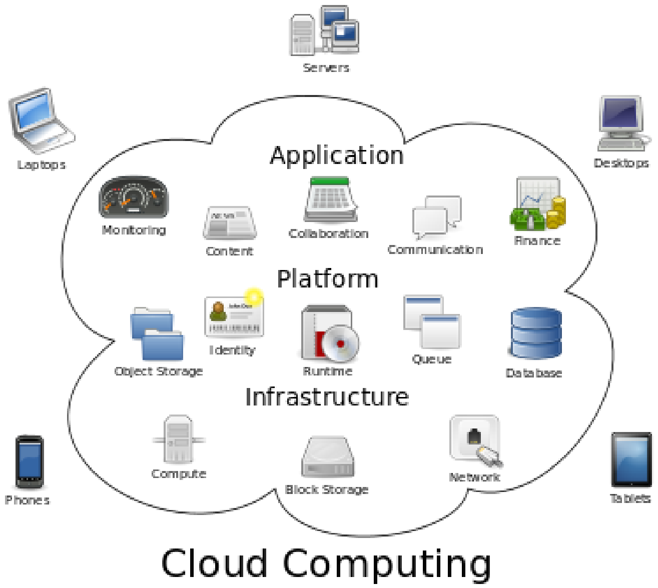


Fig 1.1 The Cloud Metaphor
Source: https://en.wikipedia.org/wiki/Cloud_computing

1.3 Types of Cloud

1. Software as a Service (SaaS)

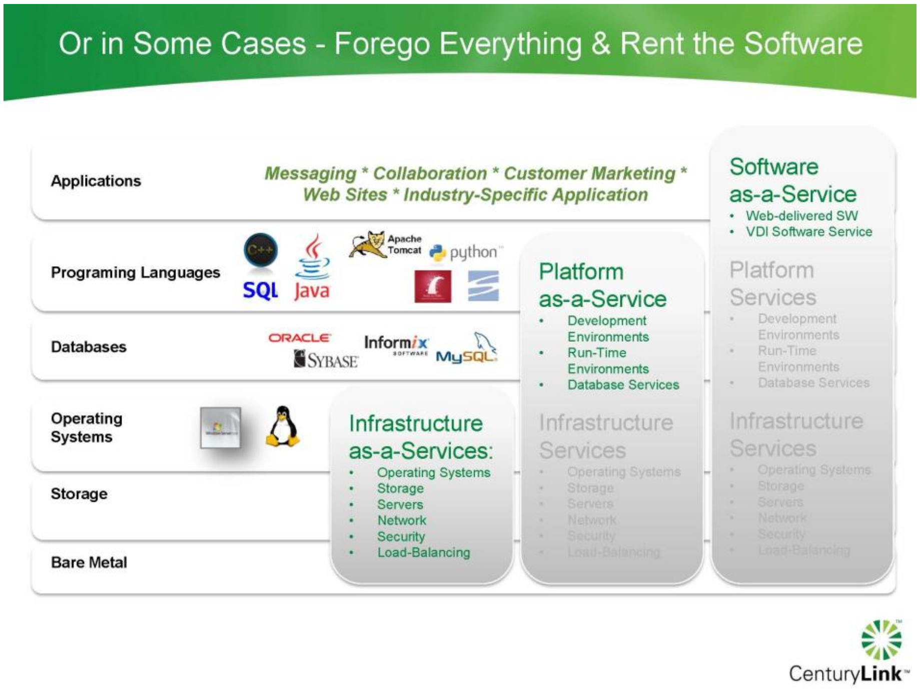
In an October 2009 publication, Peter Mell and Tim Grance of the U.S. National Institutes of Standards & Technology (NIST) defined Software as a Service (SaaS)[31] as the computing application, whereby a consumer uses the provider’s software applications running on a cloud infrastructure. An example of SaaS would be online tax filing, Remita (for Treasury Single Account, TSA in Nigeria), GIFMIS, etc. See Fig 1.1.

2. Platform as a Service (PaaS)

PaaS provides the cloud consumer with the capability to deploy applications onto the cloud platform using programming languages and tools that are supported by the cloud provider. Microsoft™ Azure and Google App engine are examples of PaaS. This is illustrated in Fig. 1.1.

3. Infrastructure as a Service (IaaS)

IaaS is the mode where the cloud user has the most control of the three types of clouds. Refer to Fig 1.1. The user has the freedom to provision processing, storage, networks, and other fundamental computing resources, where the consumer is able to deploy and run arbitrary software such as operating systems and applications. Amazon EC2 or vCloud are examples of IaaS.



Or in Some Cases - Forego Everything & Rent the Software

Applications

Messaging * Collaboration * Customer Marketing * Web Sites * Industry-Specific Application

Programing Languages

Databases

Operating Systems

Storage

Bare Metal

Infrastructure as-a-Services:

- Operating Systems
- Storage
- Servers
- Network
- Security
- Load-Balancing

Platform as-a-Service

- Development Environments
- Run-Time Environments
- Database Services

Infrastructure Services

- Operating Systems
- Storage
- Servers
- Network
- Security
- Load-Balancing

Software as-a-Service

- Web-delivered SW
- VDI Software Service

Platform Services

- Development Environments
- Run-Time Environments
- Database Services

Infrastructure Services

- Operating Systems
- Storage
- Servers
- Network
- Security
- Load-Balancing

Fig. 1.2 Delivery Modes Of Cloud Technology (Types)

Source: “Avoiding 'Cloud Failures' – Strategies to Use the Cloud Effectively” - Martin Capurro [51].

1.4 Cloud Deployment Forms[31]

A CSP or user, will always deploy or engage one or more of four cloud forms. It could be Private cloud, which is the form where cloud infrastructure is operated solely for an organization (may be managed by the organization or a third party, and may exist on premises or off premises). It could also be a Community cloud, a Public or a Hybrid cloud. It is community when the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g. a mission etc), where it is managed by the organizations or a third party and may exist on premise or off premise.

It is public, if it is available to the general public or a large industry and is owned by an organization selling cloud services. Hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). See Fig 1.2. These definitions were given in 2009 by the NIST of the US.

1.5 Cloud Security

From the foregoing, cloud computing holds a lot of promise for business in the near future. However, its benefits and implementation present concurrent challenges to both clients and providers. These include problems such as trusting vendor's security model, obtaining support for investigations since data is not with the user, loss of physical control of content by customer and inability to intervene in an event of a system failure.

The biggest among these problems is security. To hand over important data to another party (for contracted or outsourced services) is worrisome. Even in corporate organizations, where cloud computing is implemented locally, there is the likelihood of connectivity to the internet, thereby introducing the risk of unauthorized access.

In any information system, three fundamental elements are necessary for security health: confidentiality, integrity and availability. Confidentiality is protecting information from being exposed to unauthorized persons. Integrity is to ensure that information is accurate, valid and complete, by protecting it against corruption or degradation; while availability is ensuring prompt access to information when and where needed. They are known as the CIA Triad, forming the foundation for electronic information security[43].

Cloud computing security is a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. It is the most well-known challenge among users (In Fig 1.3, 74.8% of 244 repondents rated security very significant).

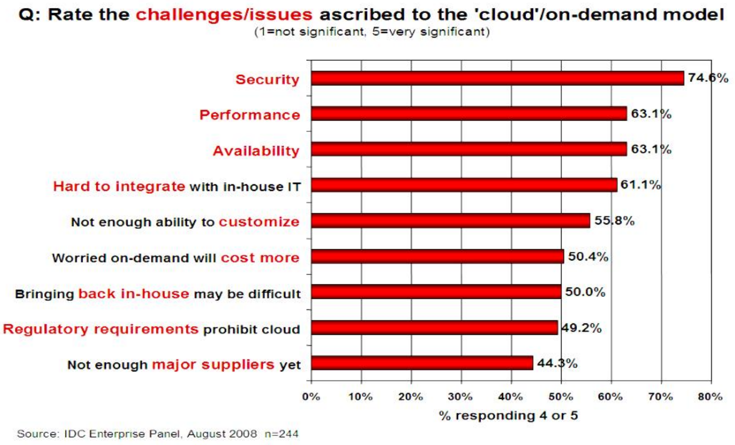


Fig 1.3 Chart Showing the Import of Security

Source: IDC Enterprise Panel, Aug 2008

The intending user of a cloud system has to be identified and given access to what and where he is entitled to and no more (authentication and authorization). Logs of past transactions must be kept, in case the need to trail an event arises.

Existing cloud services, like any other computer networks, are prone to cyber-attacks. These include:

1. Side channel attacks: where information is gained from the physical implementation of the cryptosystem rather than brute force attack.
2. Denial of service attack: where a network is brought to its knees by flooding it with useless packets.
3. Man in the middle attack: This attack takes place when the attacker places himself between two users. The attacker modifies the data shared between the two users.
4. Authentication Attacks: Most service providers use username and password for authentication purpose. The attackers use phishing models to crack the username and password[45].

1.6 Problem Statement

Based on investigations being carried out in this project, authenticating users has been found to be the biggest challenge, since the system will remain safe, if an unauthorised user is prevented from gaining access either to data in motion or at rest, as well as to application software and infrastructure. Research shows that several attempts have been made by service providers to achieve effective user authentication. The technologies deployed include the one, two, or three-factor authentications, which respectively assess one, two or three of the following schemes:

i. Something the user possesses (e.g. token or phone)

ii. Something the user knows (e.g. password or PIN)

iii. Something inherent to the user (e.g. biometrics)

The number of the schemes assessed to authenticate the user will define what is referred to as the one, two or three-factor authentication.

One and two-factor authentication models are in popular use. Based on the insight from the literature review of this research (Chapter Two), it has been found that little use has been made of the three-factor model. Therefore, the three-factor authentication model will be investigated in this work, with a view to seeing its suitability and putting forward additional options for securing cloud systems, using user authentication.

1.7 Motivation

Information, data and network securities are hot topics in contemporary technological world, even among ICT businesses. With the advent of cloud technology, which the Nigerian Government now deploys for governance, the security of the system is of interest. Many news reports reveal that there have been so many financial losses in Nigerian banks due to cybersecurity breaches and ATM card frauds. These have motivated a desire to research into this area, in order to add to knowledge and provide possible solution towards mitigating unauthorized access into clouds, as we have in banks and other online service providers.

1.8 Aims and Objectives

The objective of this thesis is to analyse some existing secure user authentication models, view them in the light of one- or two- factor authentication technique, identify their downsides and come up with a more secure three-factor model. The thesis is further expected to accumulate cloud computing security (and other) knowledge to provide a reference for further works in the same or related areas of research.

1.9 Scope

The focus of this work is on user authentication improvement. Various authentication models will be studied, criticized, and attempt will be made to identify possible improvements, through the three-factor authentication model as earlier defined. Other authentication models improvements will not be considered. Solution to privacy will not be considered and higher (or lower)-factor authentication models are also beyond the scope of the project.

1.10 Methodology

This research will test the proposed model by mathematically investigating the numerical value of the accessibility probability when an intruder attempts to gain access to a cloud system designed with a three-factor authentication model. The entropy values will be estimated for one-, two- or three-factor authentication parameters, after converting passwords, tokens and biometric inputs into numerical codes. This is expected to give an idea of the randomness (i.e. “hardness”) of the model, to an intruder.

Various log-in simulations will be used as general test data. Test results will be analysed and an inference drawn from the analyses.

1.11 Thesis Outline

This thesis consists of the introduction chapter, where the background is introduced; the motivation, aims and objective of the project, problem statement and project scope are also discussed. Chapter Two deals with an extensive literature review, while Chapter Three presents the methodology of the project. Chapter Four is a report of the experimentation on the model under investigation. Chapter Five highlights the testing results analyses, discussion, observations and summary, while Chapter Six features the project conclusions, recommendations and limitations.

Chapter 2

LITERATURE REVIEW

2.1 Severity of Cloud Security

Two customers of Citizens Financial Bank (in Northwest Indiana and the Chicago area) Marsha and Michael Shames-Yeakel fell victim to identity theft when an unknown person gained access to their online account and stole $26,500 from a home equity credit line[2]. The bank deployed a cloud computing facility for online banking but experienced a security breach.

While cloud security concerns can be grouped into any number of dimensions (Gartner named seven, while the Cloud Security Alliance identified fifteen areas of concern[6]), these dimensions have been aggregated into three general areas: Security and Privacy, Compliance, and Legal or Contractual Issues.

This research work is focused on security aspect of the challenges in cloud computing.

To be considered protected in a cloud, data from one customer must be properly segregated from that of another; it must be stored securely when “at rest;” and it must be able to move securely from one location to another.

Cloud providers have systems in place to prevent data leaks or access by third parties [29].

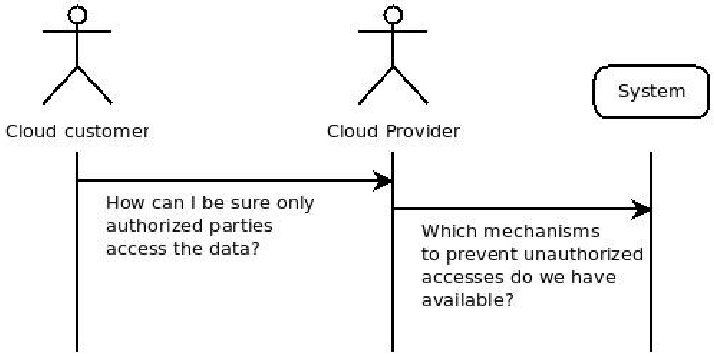

Cloud customer
Cloud Provider
System
How can I be sure only authorized parties access the data?
Which mechanisms to prevent unauthorized accesses do we have available?

Fig. 2.1 System Access Security Diagram

Source: [45]

The security issues in discussion are being addressed by various attempts from both industry and research outputs. For example, SecureCloud was developed by CA (an American IT firm) to alleviate data security and privacy risks associated with deploying information into any cloud computing environment. Its patented key-management technology combined with industry standard encryption allows businesses to control access to sensitive data stores and operate safely in public, private and hybrid clouds[32].

Companies currently working on or offering cloud security solutions include Novell, Ping Identity, Sentrigo, Symplified, and TriCipher[3] among many others.

The best way to secure a cloud is to prevent unauthorised access ab initio. This is illustrated in Fig 2.1. Unauthorised access is usually checked using authentication and authorization.

2.2 Review of Past Works on User Authentication

Authentication is the establishment of confidence in the validity of a claimant's presented identifier, usually as a prerequisite for granting access to resources in an information system [3]. Authentication is the first step in access control. On the other hand, authorization is granting access to only those parts or items of the information system, to which the user is entitled.

In researching into access security, this research work intends to focus on an authentication model.

Authentication can involve something the user knows (e.g., a password), something the user has (e.g., a smart card), or something the user "is" (e.g. a fingerprint or voice pattern). Single-factor authentication uses only one of the three forms. Two-factor authentication uses any two of the three forms and three-factor authentication uses all three forms. Using additional factors makes unauthorised access more difficult for any intruder to gain to the system [3].

2.2.1 Password-Based Authentication

One of the most popular authentication models is the use of passwords in various ways. A password is a secret (typically a character string) that a claimant uses to authenticate his identity [17]. Another specialised form of password is known as a passphrase. This is a relatively long password consisting of a series of words, such as a phrase or a full sentence. "Iamdefinitelyyour#1fan" is an example of a passphrase [5].

Users are authenticated to different strengths, using various models. This is termed the Level of Authentication, or Level of Assurance (LoA)[47]. For example, username-password model is weaker than smart card authentication.

All models that are password-dependent such as above, are subject to four major threats: password capture such as a keylogger will do, password exploitation, password replacement, and reuse of compromised passwords [1].

A password-less user authentication concept was originally proposed by IBM in the late 1980s. It actually offers the automatic generation of the password and this auto-generated password is then used to authenticate the user. In this case, the user does not require defining or remembering passwords (as the system generates the password dynamically) and the service provider does not need to store the password on his server to aid recovery of the password by the user[8]. As the password for the identity is being generated on the fly, it need not be stored anywhere and thus making the identity highly secured and device locked.

Already many online security, identity and access management (IAM) solution providers have started offering solutions based on this concept but most of them have been expensive for the end user or impractical for mass deployment and certainly not (yet) for the cloud.

2.2.2. Transaction Authentication

This authentication looks for logical flaws by comparing known user data with the details of an on-going transaction. For example, a user who lives in Japan purchases some items online, logged in from an IP address from a foreign country; this would require additional verification procedures to be sure the purchase is genuine[37]. In operation, this method of authentication usually requires the user to use additional steps such as secret question. At the present level of development, transaction authentication is not yet quite applicable on service interfaces (non-computer machines such as ATM).

2.2.3 Token Authentication.

Tokens are physical devices that are used to access secure systems. They can be in the form of a card, dongle, or Radio-Frequency Identifier (RFID) chip. RSA (an American computer network security company)'s SecureID token is about the most common in use presently. It generates an OTP (one time password) on its LED screen which users must input along with their normal username/password to access a network[37]. The down side of this is that a user will be under tremendous stress if the dongle or card is missing of forgotten at the point of need.

2.2.4. Out-Of-Band (OOB) Authentication

To harden authentication, OOB uses a separate channel (such as a mobile device) to authenticate a transaction originated from a computer. A set threshold is reached (e.g. large money transfer) before a second channel is triggered, through say, a phone call, text or notification on a specalised software application, which will request for further authorisation for the transaction to go through[37]. This model puts the user under pressure of carrying additional device along, to receive the notification for further authentication; it also necessarily creates a delay before transactions are carried through. Besides, a smart fraudster may carry out transactions (such as cash withdrawals) below the threshold, thereby avoiding the triggering. It is better if unauthorized access is made completely impossible.

2.2.5 Smart Card Authentication

A smart card is a credit-card sized card that has an embedded certificate used to identify the holder. The user can insert the card into a smart card reader to authenticate the individual. Smart cards are commonly used with a PIN (personal identification number, somewhat like a password) thereby providing multi-factor authentication. In other words, the user must have something (the smart card) and know something (the PIN). Fraudsters have however been able to clone cards (generic) that they can use to obtain access to information systems, such as ATM.

For the convenience of the user, a multiple PIN scratch-off card can be issued, where the user scratches off and each is then used only one time to log in. This lowers cost as an OTP option than tokens [38].

2.2.6 Trusted Third Party Authentication

A researcher introduced a model called Trusted Third Party. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with single sign-on (SSO) and lightweight directory access protocol (LDAP), to ensure the confidentiality, integrity and authentication (CIA) of involved data and communications[33]. However, this solution presents users with a lot of complexities and may not be preferred by many.

2.2.7 Physical Access Control

Another access security model in use by cloud service providers (CSPs), is by ensuring that physical machines are adequately secure and that access to these machines as well as all relevant customer data is not only restricted but that access is documented[6]. However, physical security cannot guarantee the security of data and applications on any system connected to a public network, such as the internet.

2.3 Multi-Factor Authentication (MFA)

MFA is really a blanket term that describes an authentication scheme that uses two or more independent sources to verify an identity, like:

1. Something possessed, as in a physical token or telephone
2. Something known, such as a password or mother's maiden name
3. Something inherent, like a biometric trait mentioned earlier

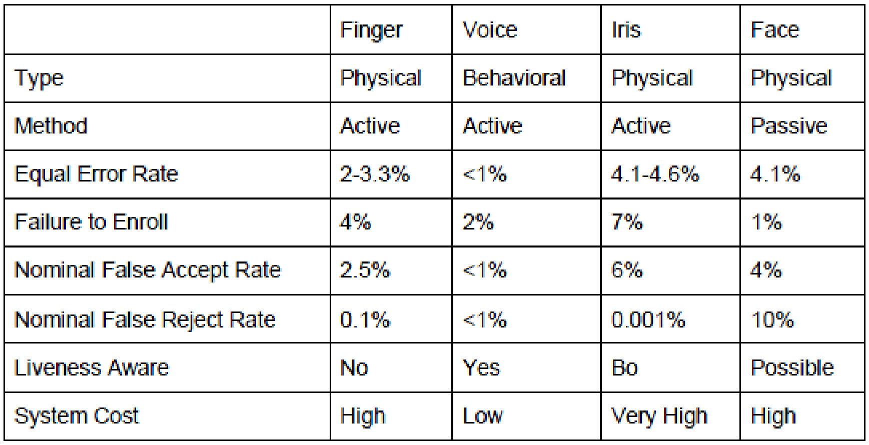
A classic example of multifactor authentication would be an ATM machine, which requires something possessed (the debit card) with something known (the PIN number) to authorize a transaction.

Biometrics literally means "measuring life," and refers to the use of known and recorded physical traits of a user to authenticate their identity, as no two individuals share the same exact physical traits. Common schemes include:

1. Voice recognition
2. Fingerprints
3. Face scanning and recognition
4. Eyeprints, such as retina and iris scans
5. Hand writing
6. Hand geometry
7. Earlobe geometry

The issue with biometrics is that, apart from voice recognition, which can be performed using a normal cell phone, they require the use of specialized scanners [37]. This technology is however being given more attention now, because computing devices are now more robust and their technologies are more granulated. More findings have shown that various biometric authentication schemes on human have different performances as shown in Table 2.1.

Table 2.1 Estimated Performances of Common Biometric Authentication Systems



	Finger	Voice	Iris	Face
Type	Physical	Behavioral	Physical	Physical
Method	Active	Active	Active	Passive
Equal Error Rate	2-3.3%	<1%	4.1-4.6%	4.1%
Failure to Enroll	4%	2%	7%	1%
Nominal False Accept Rate	2.5%	<1%	6%	4%
Nominal False Reject Rate	0.1%	<1%	0.001%	10%
Liveness Aware	No	Yes	Bo	Possible
System Cost	High	Low	Very High	High

Source: [56]

Many laptops include fingerprint readers and fingerprint readers are also available on USB flash drives.

Table 2.2 Comparison Table of Security Models Used By Leading Cloud Providers

SN	Company Name	Security Practices	Weakness
1	Amazon	SSL Encryption, Hypervisor	Software cloning possible
2	Microsoft	VPN, Identity Management, SSL Encryption.	Number of factors not efficient
3	Sales force	Intrusion Detection Systems, TLS encryption, SAML, MD5.	Software cloning possible
4	IBM	SLA, Third Party Auditor, SSL Encryption, VPN.	Software cloning possible. Third party come with its own security burdens
5	VASCO	DIGIPASS Pack for Remote Authentication, with Identikey**.**One-Time Password and e-signature validation	Only two factors. Password can be obtained fraudulently
6	Symantec	Validation & Identification Protection (VIP); Two-Factor and Risk-Based Token-less Authentication	Two factors of authentication are inefficient
7	RSA	RSA Authentication Manager; hardware tokens, software tokens, risk-based, and on-demand Short Message Service (SMS)	Weak reporting, physical tokens may be separated from user. Hardware requirement rather high.
8	CA	Strong authentication; OTP, Knowledge-Based Authentication (KBA),	Weak reporting, only Two Factors which are not effective

Sources: [36][49] [50] [51] [52] [53]

Several MFA products are compared in Table 2.2. None of the MFA products deliver all three authentication factors.

2.3.1 Three-Factor Authentication (3FA)

A combination of the three factors of authentication will lower the likelihood of unauthorized access into a cloud. For this reason, the focus of this research work is the three-factor authentication. 3FA is the use of identity-confirming credentials from the three separate schemes of authentication factors that were discussed in section 2.3. They are further referred to as the knowledge, the possession and the inherence categories [40].

It is unlikely that an attacker could successfully fake or steal all three elements involved in 3FA, which makes for a more secure log in.

Three-factor authentication will find more applications in businesses and government agencies that require high degrees of security. The use of at least one element from each category is required before a system can be considered a three-factor authentication system. Note that selecting three authentication factors from two categories qualifies only as two-factor authentication (2FA). The reliability of authentication is affected not only by the number of factors involved but also how they are implemented. In each category, the choices made for authentication rules greatly affect the security of each factor. Poor or absent password rules, for example, can result in the creation of passwords like "guest," which completely defeats the value of using a password. Best practices include requiring inherently strong passwords that are updated regularly. Facial recognition systems can in some cases, be defeated by holding up a picture. More effective systems may require a blink or even a wink to register [40]. Lax rules and implementations result in weaker security; alternatively, better rules can yield better security per factor and better security overall for multifactor authentication systems.

From the above literature review, it can be noticed that most of the security challenges are not solved by any single existing solution.

This thesis will therefore attempt to put forward an improvement on authentication, by mathematically experimenting on a three-factor authentication model using password, scratch card and biometric, and then analysing the result to draw some conclusions.

Chapter 3

METHODOLOGY

3.1 General Approach

Having shown that the popular 2-factor authentication model, though well accepted, has become insufficient with threatening security inadequacies in cloud systems, the literature review showed that there remains ample opportunity to explore 3-factor authentication.

This chapter will explain how the acceptability of the probability and entropy values that could be obtained in 3-factor model was obtained, for a potential intruder into a cloud computing environment, who tries to guess the authentication credentials correctly. An interface was designed in Java to illustrate three authentication credentials (three factors) expected to return a “pass” or a “fail”. This is exemplified in Fig 3.1 . The three factors chosen are password (minimum of eight digits), card code (16 digits) and a fingerprint field. The fingerprint data is usually coded numerically.

It is hoped that future researchers will be able to configure a prototype of the technology through a client-server architecture environment to be created using Remote Authentication Dial-In User Service (RADIUS) server application installed to authenticate users on a Local Area Network (LAN) of say, three computers using CAT 6 UTP cabling with a switch and a computer to function as server.

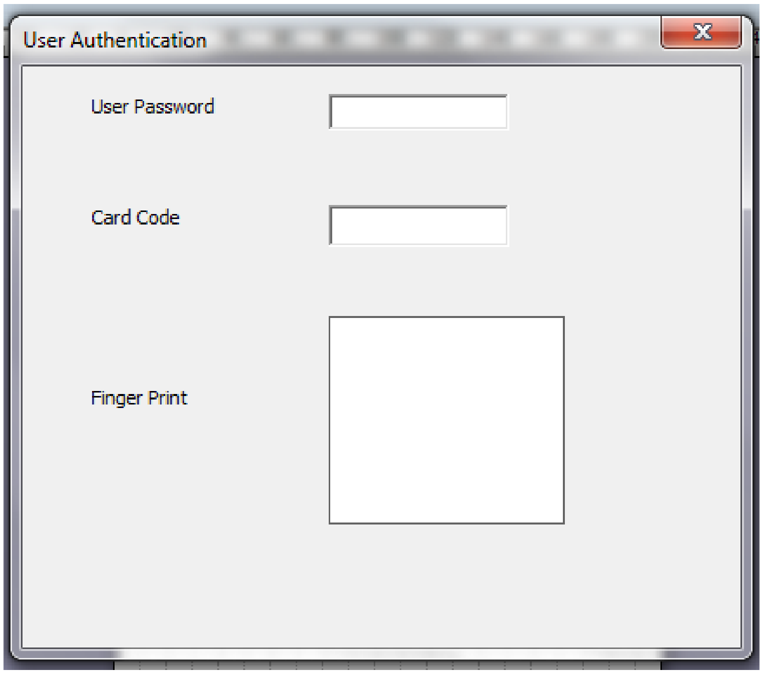


Fig. 3.1 A Model User Authentication Interface to Implement 3-FA

See Appendix I – IV for the design and source codes of the 3-FA model developed.

3.2 User Authentication Probability Equations

Mathematically,

a. For the first authentication factor, 1-FA (password),

if we limit number of characters to be entered, to 8 (number and letters only), with case sensitivity, First Sample Field (lowercase letters of the alphabet)

$SF_1 = 26$ ……………..… (3.1)

2nd Sample Field (uppercase letters),

$SF_2 = 26$ ……..…..……... (3.2)

3rd Sample Field (numerals 0 – 9),

$SF_3 = 10$ ………...……... (3.3)

These will form a single sample field:

Total Sample Field

$SF_t = SF_1 + SF_2 + SF_3 = 62$……... (3.4)

We define a formula when selecting r items from n items, allowing repetition,

$C(r+n-1,r) = C(r+n-1, n-1)$ …… (3.5) [58]

Where r = No of selection, allowing repetition,

n = No of items to choose from.

This can otherwise be written as

$${}^{(r+n-1)}C_r = \begin{pmatrix} r+n-1 \\ r \end{pmatrix} = ((r+n-1)! \div r!) \div (n-1)! \quad \text{….(3.6)} \ [4]$$

Note that, conversely, the number of different combinations of n different items, taking k at a time, without repetition, is

$$\begin{pmatrix} n \\ k \end{pmatrix} = (n! \div k!) \div (n-k)! \text{……………………….(3.7) [4]}$$

Going back to equation (3.1) to (3.6):

Taking any 8 texts together from a sample field of 62,

$$^{69}C_8 = \begin{pmatrix} 69 \\ 8 \end{pmatrix} = 69!/8!/61! = 8361453672 \text{ ways……(3.8)}$$

So, there are 8361453672 ways of selecting ANY 8 texts from 62, allowing repetition, for the password.

b. For the second factor, in a 2-FA, adding a scratch card with 15-digit assigned code (15 digit numbers only)

Taking ANY 15 digits together (allowing repetition, since there are only 10 numbers), according to equation (3.6)

$$^{24}C_{15} = \begin{pmatrix} 24 \\ 15 \end{pmatrix} = 24!/15!/9! = 1307504 \text{ ways……..…(3.9)}$$

That is, there are 1307504 ways selecting numbers to be on the card.

c. In a 3-FA, the third factor, a finger print, is usually treated by conversion into binary digits (encoding). If the encoded value (the stored recognised value, not the instantaneous sampled value) of finger print is taken considering a 128 by 64 quantized system, at a sampling of 8 by 8,

   The sampling field has a total bit of 128*64 = 8192, while the sampling rate (number of selections) is 8*8 = 64;

   Without repetition, the number of 8 by 8 plates that can be found in a 128 by 64 is

   8192/64 = 128

   The Probability of any event X, is given by

   P(X) = No of times X occurs ÷ No of samplings……..(3.11)

The probability of an intruder guessing right in a 2-factor authentication (password and card code) under this consideration is

P(Auth, 2-fac) = (1/8361453672) X (1/1307504)

- since it is a combination

= 9.14693 e-17

P(Auth 3-fac) = (1/8361453672) X (1/1307504) X (1/ 128)

= 7.14604 e-19

The Guessing Entropy of the intruder is calculated using

$$H=(-1/p)\log(p) \ldots\ldots\ldots\ldots\ldots\ldots (3.12)$$ [3]

Where p is the probability value of guessing success.

Introduction of the third factor will greatly reduce the chances of a correct combinatorial guess as follows:

Based on how it applies in this investigation, entropy means the degree of uncertainty in the value of a password or the ”hard-to-predict” quality. The conventional expression of entropy of passwords is in bits.

For the 2-FA, Guessing Entropy will be

$$H = (-1/9.14693\text{ e-}17) \log (9.14693\text{ e-}17)$$

$$\approx 1.75345\text{ e+}17$$

For the 3-FA as considered above, the Guessing Entropy will be

$$H = (-1/7.14604\text{ e-}19) \log(7.14604\text{ e-}19)$$

$$\approx 2.5393\text{ e+}19$$

The entropy is much higher for 3-FA than 2-FA comparatively making an intruder encounter much more difficulty guessing the credentials.

Chapter 4

EXPERIMENTS AND RESULTS

4.1 Test Equations

In Chapter 3 of this thesis, certain equations were established, which will be used extensively in this chapter:

i. Selection of r items from n items, allowing repetitions:

$$^{(r+n-1)}C_r = \begin{pmatrix} r+n-1 \\ r \end{pmatrix} = ((r+n-1)! \div r!) \div (n-1)!$$

ii. Probability of occurrence of X:

P(X) = No of times X occurs ÷ No of samplings

And for serial or chain events,

P(X,Y,Z) = P(X) * P(Y) * P(Z)

iii. Guessing Entropy of any combined credentials:

H=(-1/p)log(p)

Taking a look at the 1-FA, the 2-FA and the 3-FA, a table can be generated, of the probability values of intruder succeeding by guessing the password, as well as the corresponding guessing entropies. These data is shown in Table 4.1.

4.2 Probability Calculations

Using the equations in section 4.1, data can be generated as given in Table 4.1 below:

Table 4.1: Comparison of Probability Values and Guessing Entropies for 1-FA, 2-FA and 3-FA

No of Characters Entered As Password	1-FA		2-FA		3-FA	
r1	n1 = 62		n1=62; n2=10; r2=15		n3=8192; r3=64	
	P(1-FA)	**H(1-FA)**	**P(2-FA)**	**H(2-FA)**	**P(3-FA)**	**H(3-FA)**
2	5.1203E-04	6.4260E+03	3.9161E-10	2.4022E+10	3.0595E-12	3.7635E+12
3	2.4002E-05	1.9248E+05	1.8357E-11	5.8486E+11	1.4341E-13	8.9556E+13
4	1.4770E-06	3.9476E+06	1.1297E-12	1.0576E+13	8.8254E-15	1.5925E+15
5	1.1190E-07	6.2122E+07	8.5579E-14	1.5270E+14	6.6859E-16	2.2697E+16
6	1.0021E-08	7.9828E+08	7.6638E-15	1.8418E+15	5.9874E-17	2.7095E+17
7	1.0315E-09	8.7119E+09	7.8892E-16	1.9144E+16	6.1635E-18	2.7923E+18
8	1.1960E-10	8.2965E+10	9.1469E-17	1.7535E+17	7.1460E-19	2.5393E+19

Where

n1 - Sample field of first factor (password)

r1 - No of characters selected together

n2 – Total sample field of second factor (Card code)

r2 – No of digits on a typical card

n3 – Total number of pixel/pattern plates possible for finger print capture

r3 – No of pixel in one pattern plate

P(1-FA) – Probability of correct guess in a 1-Factor Authentication (password)

P(2nd Fac) – Probability of correct guess on the Second factor only (card code)

P(2-FA) – Probability of correct guess in 2-Factor Authentication

= P(1-FA) * P(2nd Fac)

P(3rd Fac) – Probability of correct guess on the Third factor only (finger print)

= Sampling field/sample size

P(3-FA) – Probability of correct guess in 3-Factor Authentication

= P(2-FA) * P(3rd Fac)

H(1-FA) – Entropy in 1-FA

= {(-1/P(1-FA))log P(1-FA)}

H(2-FA) - Entropy in 2-FA

= {(-1/P(2-FA))log P(2-FA)}

H(3-FA) - Entropy in 3-FA

= {(-1/P(3-FA))logP(3-FA)}

Plotting the various graphs of the given probabilities and the given entropies in Table 4.1 above, versus number of characters in the password of the first factor, Fig 4.1 – Fig. 4.6 can be deduced:

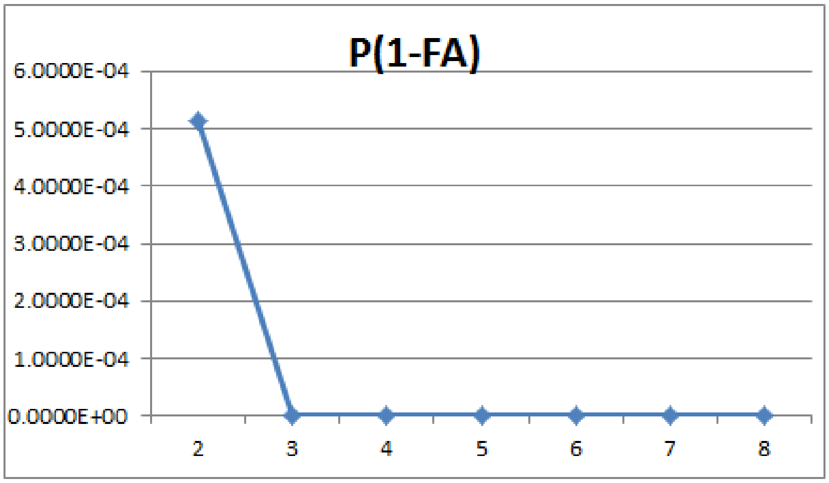


Fig. 4.1: Graph of Probability P(1-FA) versus No of Characters of Password

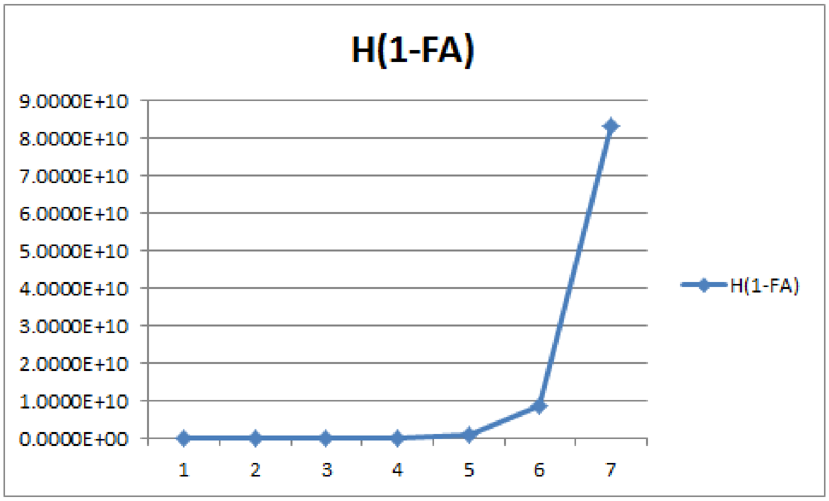


Fig. 4.2: Graph of Entropy H(1-FA) versus No of Characters of Password

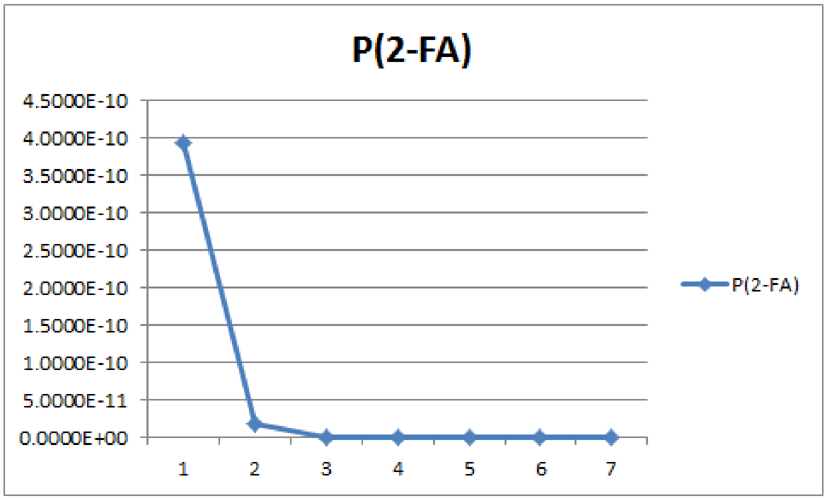


Fig. 4.3: Graph of Probability P(2-FA) versus No of Characters of Password

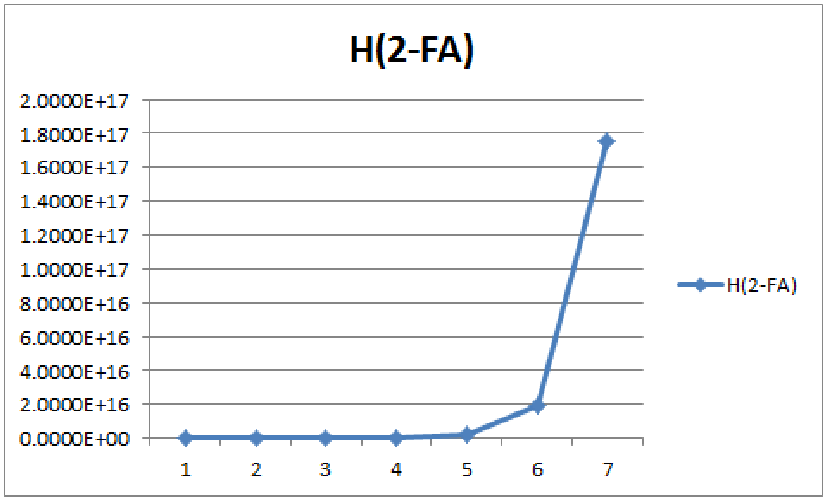


Fig. 4.4: Graph of Entropy H(2-FA) versus No of Characters of Password

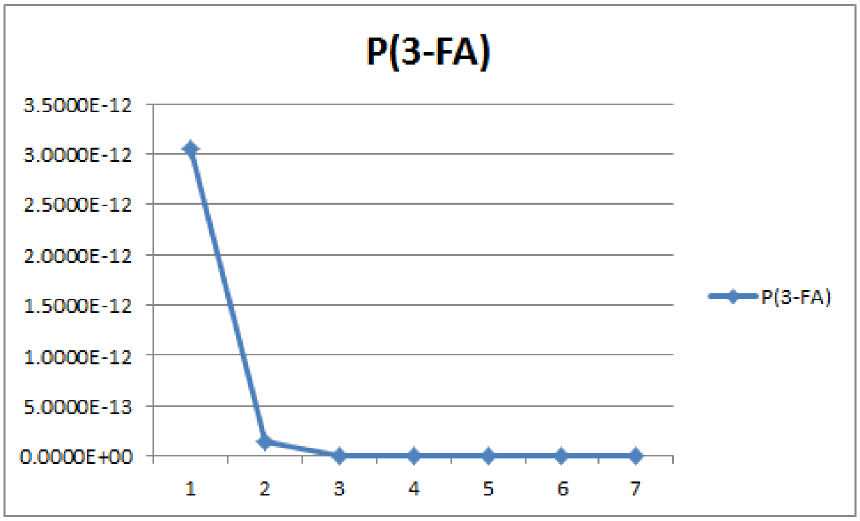


Fig. 4.5: Graph of Probability P(3-FA) versus No of Characters of Password

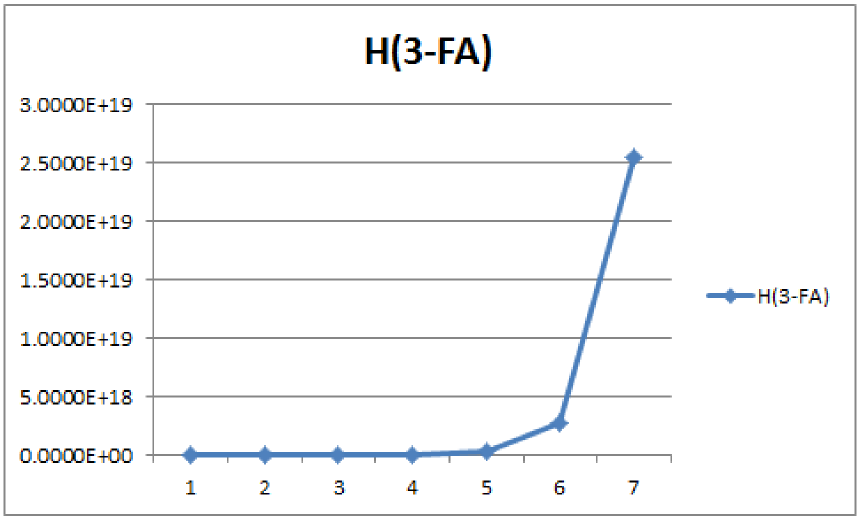


Fig. 4.6: Graph of Entropy H(3-FA) versus No of Characters of Password

Chapter 5

RESULTS ANALYSIS AND DISCUSSION

5.1 Introduction

In Chapter 4, the graphs of the intruder guess success probabilities and entropies for 1-FA, 2-FA and 3-FA were plotted, based on the corresponding data generated. Refer to Table 4.1. A study of these graphs will shed some light on the behaviour of the model under investigation. This will then guide into a conclusion.

5.2 Results Analysis

With reference to Table 4.1, we can compare the probability of an intruder correctly guessing the access password to a cloud application, using 1-FA. This is denoted as P(1-FA). Using only password factor, P decreases as the required number of password characters is increased (from 2 to 8). This is graphically shown in Fig. 4.1.

Similarly, the difficulty of the password (entropy, H(1-FA)) increases in identical manner from the same table and as shown graphically in Fig. 4.2.

However, as the factor of authentication is increased from one to two and three, there is a sharp reduction in probability of guessing right

(Table 4.1). This becomes pronounce when the number of password characters increases from 4 to 5 in 2-FA and from 3 to 4 in 3-FA. The entropies also catapult by hundreds within the mentioned ranges.

Interestingly, at 8 characters of password, the probability of correct guess in 2-FA becomes reduced by ten millionth of that of 1-FA, while that of 3-FA is reduced by over one billionth of that of 1-FA.

Fig. 4.3 to 4.6 are graphical representations of the described probability and entropy scenarios.

5.3 Discussion

From the foregoing, cloud access control becomes better when the factor of authentication is increased, more so for 3-FA model, buttressing the interest of the research. This is attested to above, by the sharp difficulty of the authentication procedure when 3-FA comes to play. The argument is also strengthened by the very low probability of guessing right calculated in Chapter 4.

5.4 Observations

In the line of this research, some observations were made based on discussions with other researchers, technology enthusiasts and solution developers in industry. These include:

i. Three-factor authentication model has many options especially in the second factor (Card Code, One-Time Password OTP to phone, Token etc) as well as in the third factor (Biometrics, see Section 2.3).

ii. Introduction of additional factors increases the computer data overhead. However, the sustained frequent emergence of advancement in computer power (speed, memory, data-read technology, storage etc) has built confidence that more powerful computers will always emerge to handle increased data overhead.

iii. Multi-factor authentication models will make economic sense when applied to valuable data/asset environments, due to the inevitable comparatively high initial costs.

5.5 Summary

In this Chapter, results generated from earlier experiments were analysed and discussion elicited based on the analysis. Other possible options that could have been considered under this work, new computer advancements and some cost considerations were mentioned in the observation.

Chapter 6

CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This research work had set out clear objectives of acquiring knowledge on cloud security, reviewing existing models for secure cloud user authentication, with a view to coming up with an additional option. It further set out to provide a reference material for further works in the same or related areas of research. Having realised the importance of this current technology to research, education, national economy, international relations, intelligence, commerce and governance, an option of secure user authentication has been investigated, which is the 3-factor authentication.

6.2 Conclusion

This investigation has found that the three-factor authentication model heavily reduced unauthorised access to cloud systems, using probability theories. It was found to be highly chaotic to a guessing intruder, making it very difficult to gain access. A user interface was proposed for implementation of the idea and the method was found to be quite feasible, especially in both industrial and valuable data asset applications.

6.3 Limitations of the Work

This work was done bearing some constraints in mind. These include the selection of only eight digits for password (first factor). Contemporary practice usually expects much longer passwords. Card code was chosen for second factor, where other choices exist, such as OTP to phone, secret questions etc. There is also the need to further extend the model to include network environments to more accurately test the circumstances surrounding an industrial deployment of the model.

6.4 Recommendations

With the observations gathered from this research, the followings are recommended:

i. Further research should be carried out to study biometrics schemes with a view to knowing which of them is better for which ever application in a 3-FA.

ii. The choice of processor to work with the authentication model in this work, should be robust, high-speed, up-to date and powerful, in view of additional data overhead upon introduction of additional authentication factor.

iii. Multi-factor authentication models will make economic sense when applied in industry to valuable data/asset environments.

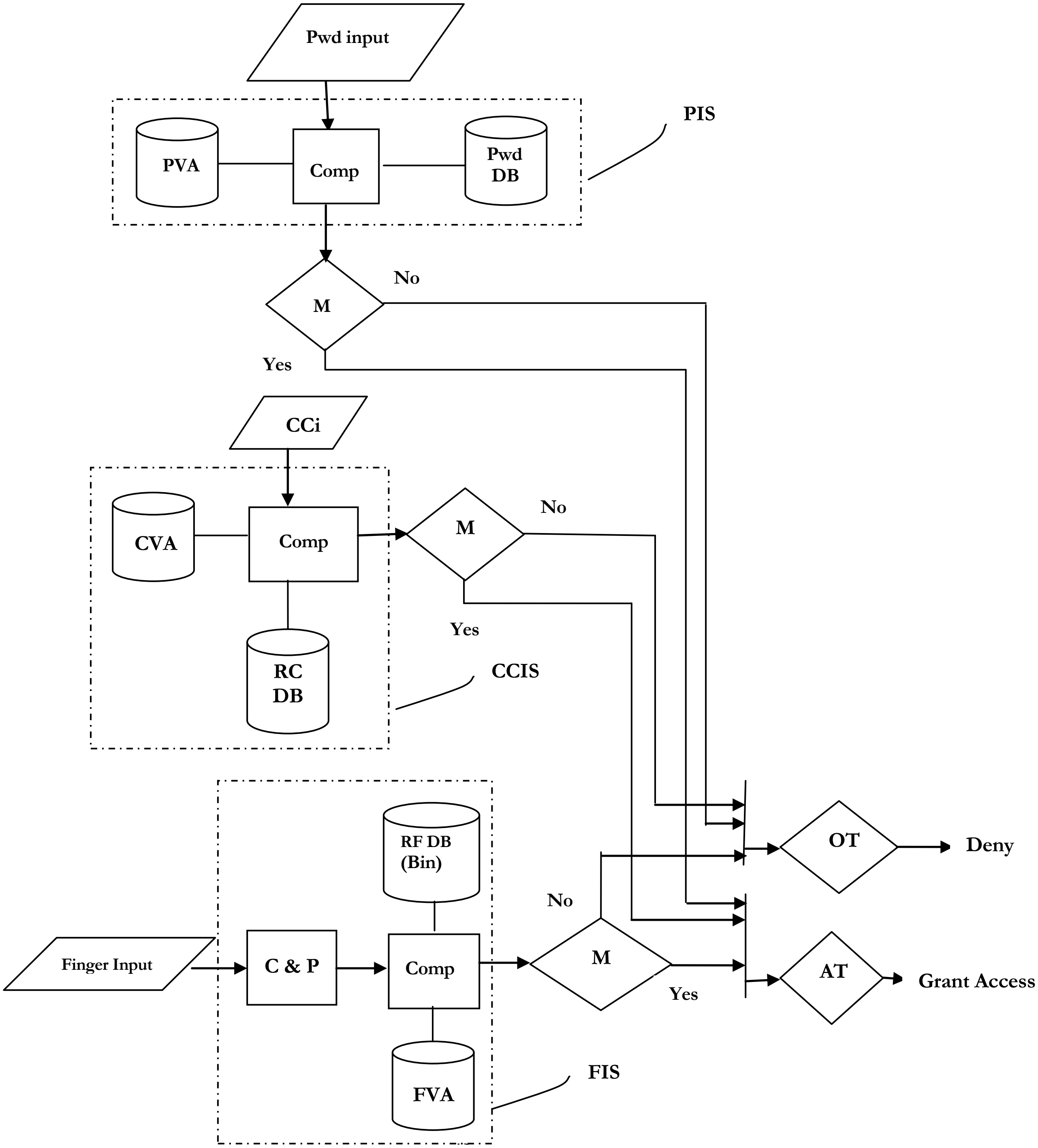
Appendix I

SOURCE CODE FOR THE MODEL USER AUTHENTICATION INTERFACE TO IMPLEMENT 3-FA (VISUAL BASIC VER. 2006)

```
Private Sub Label3_Click()

End Sub

Private Sub UserForm_AddControl(ByVal Control
As MSForms.Control)

End Sub

Private Sub UserForm_Click()

End Sub
```

Appendix II

SYSTEM DIAGRAM FOR 3-FA MODEL USING PASSWORD, CARD CODE AND FINGERPRINT FACTORS



The labels in diagram under Appendix II are:

Pwd input	=	password input stage
PVA	=	password verification algorithm
Comp	=	comparator system
Pwd DB	=	database of registered passwords
PIS	=	password identification system
M	=	matching decision
CCi	=	card code input stage
CVA	=	code verification algorithm
RC DB	=	database of registered codes
CCIS	=	card code identification system
RF DB (Bin)	=	database of registered fingerprints (converted to binary)
C & P	=	capturing and processing
FVA	=	fingerprint verification algorithm
FIS	=	fingerprint identification system
OT	=	"One True" decision module – one true input switches gate
AT	=	"All True" decision module

Operation

In the above diagram, the user inputs his password first, assuming he is already registered (was issued a password) by the service provider, to who network he belongs. The comparator, Comp compares his input with the content of the password database, Pwd DB, using a special password verification algorithm, PVA. The system uses a password identification system, PIS. If the input matches, based on M, the user's card code input is awaited, otherwise, an "access denied" is output. In the card code stage, card code input, CCi, presents the user's code to a comparator, which matches the code with the registered or pre-issued card code in the database, RC DB, using a code verification algorithm, CVA, all consisting the card code identification system, CCIS. A failure in this stage automatically denies access to the service; a success leads the system to await fingerprint identification system, FIS, stage. When a fingerprint input is seen, the fingerprint captured is specially processed by the C & P, compared by the Comp using fingerprint verification algorithm FVA, with reference to the already registered fingerprint in the RF DB, which is ready in binary format. If the matching M is true, the system ensures all other factors are still true, upon which an access to the service is granted by an "All True" decision system, AT.

Appendix III

PSEUDO CODE FOR 3-FA USING PASSWORD, CARD CODE AND FINGERPRINT

```
** Program to Authenticate a user, using a 3-Factor Authentication
 ** Technique**

Start

** Password input and verification section**
Define pwdb();     ** Password Database**
       Get PWD;

**Database accepts password class, consisting alphanumeric and special
 **characters**

compare PWD with content of pwdb();
       If  PWD ɔ pwdb()    **belongs to**
           Password=TRUE;
           Proceed to cdcdsection;
       Else    Output "Failed";

**Access card code verification section**
cdcdsection;
Define cardcode();
       Get CDCODE;

**Card Code is from service-provider-assigned card number, with range 0 – 9,
** taking 16 digits at a time**

compare CDCODE with content of cardcode();
         If CDCODE ɔ cardcode()
          Card=TRUE;
          Proceed to Fngprtsection;
        Else     Output "Failed";

**Finger Print verification section**
Fngprtsection;
Define fingerprint();
```

```
    Get FNGPRT;

**Finger Print has been converted into binary codes by a separate algorithm,
in an already registered database**

compare FNGPRT with content of fingerprint();
     If FNGPRT ↄ fingerprint()
        Biometric=TRUE;
        Proceed to Combsection;     **Combination section***
    Else   Output  “Failed”;

** Three-factor authentication combination and access decision section**
Combsection;
     If password AND card AND biometric NOT TRUE
        Output   “Failed”;
     Else  Output “Passed”;

End
```

Appendix IV

A TYPICAL SOURCE CODE FOR 3-FA IMPLEMENTATION IN MATLAB LANGUAGE

```
% Program to implement 3-Factor Authentication Technique
% ======================================================
% Password input and Verification Section
% ======================================================

Inputed_Password = input('Please enter an alphanumeric password of at least 6 characters: ','s');
% Assume chosen password is Wert12b7

Stored_Password = 'Wert12b7';

% Now to authenticate this password

for Password_entry_counter = 1:3
Password_Status = strcmp(Stored_Password, Inputed_Password);

if Password_Status == 1

   disp('Password ok!');

   break;

elseif Password_entry_counter == 3;

   break;

else

   Inputed_Password = input('Wrong Password. Please enter the password again: ','s');

end
```

```
end

if Password_Status == 1

% ======================================================
% Card Code Verification Section
% =======================================================

CardCode = input('Please enter the 16 digits card number in your card: ','s');

% Assume the actual card number is 2849 2903 3974 9933

StoredCardNumber = '2849290339749933';

% Now to authenticate this Card Number

for CardNumberEntryCounter = 1:3

CardNumberStatus = strcmp(StoredCardNumber, CardCode);

if CardNumberStatus == 1

   disp('Card Number Verified!');

   break;

elseif CardNumberEntryCounter == 3;

   break;

else

   CardCode = input('Wrong Card Number! Please reenter the card number:

','s');

end

end
```

```
end

if (Password_Status == 1 && CardNumberStatus == 1)


% =========================================================
% Finger Print Verification Section
% =========================================================


FingerPrintBinary = input('Please place your right forefinger on the fingerprint

reader: ','s');

% Assume that the actual finger print binary code extracted from a right
% forefinger is 1001011

StoredFingerPrintNumber = '1001011';

% Now to authenticate this Finger Print Binary Code

for FingerPrintScanningCounter = 1:3

FingerPrintAuthenticationStatus =
                    strcmp(StoredFingerPrintNumber, FingerPrintBinary);

if FingerPrintAuthenticationStatus == 1

   disp ('Finger Print Verified Ok.');

   disp ('You are Welcome!');

   break;

elseif FingerPrintScanningCounter == 3;

   break;

else

   FingerPrintBinary =
          input('Wrong Finger Print! Please place your finger again: ','s');
end
end
end
```

REFERENCES

1. Karen Scarfone & Murugiah Souppaya, *Guide to Enterprise Password Management* **,** Special Publication 800-118, Computer Security Division, National Institute for Standards and Technology, April 2009.

2. Marsha L. Shames, *Memorandum Opinion And Order : Case No: 07 C 5387*,Yeakel And Michael W. Shames - Yeake Vs Citizens Financial Bank, In The United States District Court, For The Northern District Of Illinois, Eastern District, August 21, 2009.

3. William E. Burr, Donna F. Dodson and W. Timothy Polk*: Electronic Authentication Guideline,* Special Publication 800-063, Version 1.0.2. (Information Security); Computer Security Division, National Institute for Standards and Technology, April 2006.

4. Erwin Kreyszig, *Advanced Engineering Mathematics*, 9th Ed. John Wiley & Sons, Inc., 2006, pg 1000.

5. Gurudatt Shenoy, Founder EasySecured™*, Identity Management in the Age of Cloud Computing*, Oct 2009.

6. Gartner: *Seven Cloud-Computing Security Risks*. InfoWorld. 2008-07-02. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

7. Carl Almond, *A Practical Guide to Cloud Computing Security,* Avanade Inc, August 2009.

8. Brodkin, Jon. *IBM Unveils 'Cloud Computing.'*, Network World. Nov. 19, 2007. Vol. 24, Iss. 45. pg. 10.

9. *IBM Introduces Ready-to-Use Cloud Computing*, IBM. Nov. 15, 2007. http://www-03.ibm.com/press/us/en/pressrelease /22613.wss.

10. Lohr, Steve. *Cloud Computing and EMC Deal*, New York Times. Feb. 25, 2008. pg. C6.

11. Infoworld Magazine; *Special Report "Cloud Computing Deep Drive*" Sept., 2009.

12. Gourley Bob "Cloud Compuing and Cyber Defense" Mar 2009, Published Crucial Point LLC.

13. Trusted Computing Group. " Cloud Computing and Security- A National Match". April 2010.

14. Wilson Charles et al "Biometric Data Specification for Personal Identity Verification" January 2009, Published by Information Technology Laboratory, National Institute of Standards and Technology (NIST).

15. Goulding, J.T. et al " Identity and Access Management for the Cloud: CA's Strategy and Vision" May 2010. Published by CA Technologies.

16. Ponemon L.(Dr), "Security of Cloud Computing Users: A study of Practitioners in the US & Europe". May 2010.

17. "NetApps, Cisco, Others Advocate Cloud Computing for Enterprise Profitability". BusinessDay Newspaper (16th March 2010).

18. "Amazon Cloud Can Hack Wifi Networks" ThisDay Newspaper (13 January 2011) Pg 35.

19. "Cloud Computing Used to Hack Wireless Passwords". ThisDay Newspaper 13 January 2011, Pg 42.

20. RSA, The Security Division of EMC (white paper): "How to Determine the True Total Cost of Ownership for Two-factor Authentication" 2010.

21. Andy Bechtolsheim "Cloud Computing" (Paper Presented), Nov., 12, 2008.

22. Schurmann T., Grassberger P.; "Entropy Estimation of Symbol Sequences". Department of Theoretical Physics, University of Wuppertal, D-42097 Wuppertal, Germany, October 1996.

23. Halbheer R. and Cavit D., “Cloud Computing Security Considerations” Microsoft, January 2010.

24. Cachin C., Keidar I. and Shraer A. “Trusting the Cloud”. ACM SIGACT News June 2009, Vol. 40 No. 2.

25. Molnar D. and Schechter S. “Self Hosting Vs Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud”. Microsoft, 2010.

26. Cloud Security Alliance$^{\mathbf{SM}}$ “Top Threats to Cloud Computing v1.0” March 2010. http://www.cloudsecurityalliance.org/topthreats.

27. Goldwasser S. and Micah S. “Probabilistic Encryption” Journal of Computer and System Sciences, vol. 28 No 2, April 1984.

28. Bhavani Thuraisingham, “Introduction to Cloud Computing and Secure Cloud Computing” (Presented Paper) University of Texas (Dallas), January 23, 2015.

29. Chunming R.,Nguyena S.T., Jaatunb M.G., “Beyond lightning: A survey on security challenges in cloud computing” Computers & Electrical Engineering,Volume 39, Issue 1, January 2013, Pages 47–54, Elsevier Ltd.

30. A. Battou et al (2010, November 5). Cloud Computing (Update) [Online]. http://csrc.nist.gov/groups/SNS/cloud-computing

31. “Addressing Data Security Challenges In The Cloud”, Trend Micro White Paper, July 2010.

32. Dimitrios Z, Dimitrios L. (2010, May) “Addressing cloud computing security issues”. Dept of Product & Systems Design Engineering, University of the Aegean, Syros 84100, Greece (Revised 2010, December 11) [Online] www.sciencedirect.com/science/article/pii/S0167739X10002554.

33. Mell P., Grance T. “Effectively and Securely Using the Cloud Computing Paradigm” NIST, Information Technology Laboratory 10-7-2009.

34. A.Sharma (2010). “The Most-Common Authentication Methods Used Today” (2016 ed.). [Online]. Available: http://www.tweakandtrick.com /2012/06/most-common-authentication-methods-used.html

35. D. Strom (2014 November), “Comparing the top multifactor authentication vendors.” [Online]. http://searchsecurity.techtarget.com/feature/The-fundamentals-of-MFA-Comparing-the-top-multifactor-authentication-products

36. Gibson D. (2011, June 6) “Understanding the Three Factors of Authentication” [Online] http://www.pearsonitcertification.com/articles/article.aspx?p=1718488

37. National Informatics Centre, Integrated Defence Staff of India, (2009, September), “Advanced authentication technique” [Online] http://ids.nic.in/tnl_jces_Sep_2009/Advanced authentication techniques.pdf.

38. Kearns D., (2007, March 28) “Seven strong authentication methods: Strong/second factor authentication methods” [Online] www.networkworld.com/article/2296774/access-control/seven-strong-authentication-methods.html

39. Rouse M., (2014, December) “Authentication factor” [Online] http://whatis.techtarget.com/definition/authentication-factor

40. Cobb M. (2009, August) “Are 'strong authentication' methods strong enough for compliance?” [Online] http://searchsecurity.techtarget.com/tip/Are-strong-authentication-methods-strong-enough-for-compliance

41. Gheorghe M.,” Investment Decision Analysis In Information Security” Revista Economică , Supplement No. 5/2012, 19th IECS 2012, University of Sibiu Pg 86 -87.

42. Kalimullah L., Ataullah M., “A Review on Cloud Computing Privacy Solutions” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013 ISSN: 2277 128X , pg. 368-372.

43. Martínez D.J., “Privacy and Confidentiality issues in Cloud Computing architectures” , Masters Thesis of the Masters in Computing, at Barcelona School of Informatics (Facultat d'Informàtica de Barcelona) of the Technical University of Catalonia 2013.

44. Anusha K.P, Shah Pritam G., “Enhanced Security Model for Cloud Using Ones compliment Re-coding for Fast Scalar multiplication in ECC” IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Vol 16, Issue 3, Ver. II (May-Jun. 2014), PP 107-112.

45. Inman G., Chadwick D. “A Privacy Preserving Attribute Aggregation Model for Federated Identity Managements Systems” University of Kent, 2009. Publication from https://kar.kent.ac.uk

46. Bhavani T., “Introduction to Cloud Computing and Secure Cloud Computing” Paper at The University of Texas at Dallas, 2015

47. Venkata S., Maddineni K., Ragi S., “Security Techniques for Protecting Data in Cloud Computing”. School of Computing Blekinge Institute of Technology Sweden, 2011 .

48. EDUCAUSE® (2009, August 3) **“**Seven Things To Know About Cloud Computing”, [Online] https://library.educause.edu/~/media/files/library/2009/8/est0902-pdf.pdf

49. Martin Capurro , *Avoiding 'Cloud Failures' – Strategies to Use the Cloud Effectively ,Product Management & Development.* CenturyLink Dedicated Hosting & Cloud Services. Santa Clara – June 2011.

50. RSA (US) 2016 “RSA Authentication manager” [Online] https://www.rsa.com/en-us/products-services/identity-access-management/securid/authentication-manager

51. Symantec Corporation (2015, July)“Symantec™ Validation and ID Protection Service” © 2015, [Online] https://www.symantec.com/ content/dam/symantec/docs/data-sheets/validation-and-id-protection-service-en.pdf

52. CA Technologies Datasheet (2015) “CA Strong Authentication” [Online] http://www.ca.com/us/securecenter/ca-strong-authentication.aspx

53. VASCO Data Security International (2016) “DIGIPASS Authenticators” https://www.vasco.com/products/two-factor-authenticators/index.html

54. William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk “Electronic Authentication Guideline” NIST,Computer Security Div., Information Technology Laboratory. NIST.SP.800-63-2, Aug., 2013

55. Stephens B. (2011, Fall) Course Notes; “CMSC 203, Discrete Structures” Dept of Comp. Science & Electrical Engineering, University of Maryland, Baltimore County. [Online] http://www.csee.umbc.edu/~stephens/203/PDF/6-5.pdf

56. Jung S.M. “Design of Low Power and High Speed CMOS Fingerprint Sensor” International Journal of Bio-Science and Bio-Technology Vol.5 No.2, April, 2013